PKWARE

pkware.com

Simplifying GDPR Compliance

Non-Compliance Comes at a Cost

2021

Contents

Non-Compliance Comes at a Cost

The General Data Protection Regulation (GDPR) may have been created in the European Union (EU), but this consumer privacy law applies to any organization, anywhere in the world, that controls or processes the personal data of EU residents. Enforced as of May 25, 2018, GDPR is designed to increase EU individuals' control over their personal data as well as increase accountability for businesses that hold personal data.

In keeping with the law's central concepts of data protection by design and default, organizations are required to build strong data security measures into their products and services and to follow strict guidelines as to how personal data may be used. Fines for non-compliance could reach as high as 4 percent of an organization's annual revenues or €20 million, whichever is higher. A high-risk data breach resulting in additional reputational and legal damages could cost even more.

As of January 2021, more than $330 million USD (€272.5 million) in fines have been imposed for a wide range of infringements across the 27 EU member states, plus the UK, Norway, Iceland, and Liechtenstein, according to a recent report by international law firm DLA Piper.[1] Most notably, the French privacy regulator CNIL handed out a €50 million fine to Google for its data handling practices; Germany fined retailer H&M €35.2 million for keeping improper records of employee personal activities at a call center; and Italy issued a €27.8 million fine to telecommunications operator Italian Telecom for its data handling and marketing activities.[2] The DLA Piper report also notes that a "failure to implement appropriate security measures" is among the most common reasons for GDPR fines thus far.[3]

GDPR Compliance is an Organization-Wide Effort

The GDPR is a massive piece of legislation covering a wide range of rights and responsibilities; yet, apart from suggesting encryption, it does not explicitly outline how to achieve and maintain compliance. Most requirements are directed at data controllers: businesses that determine how and when personal data is collected, stored, used, or transmitted. But the law also sets rules for data processors, which are businesses that collect or manage data on behalf of a data controller.

Many of the GDPR's main concepts and principles are similar to those in its predecessor, the 1995 Data Directive, but there are additional requirements and enhancements that will require new and different processes. (Read the full text of the law.) For organizations, the key GDPR requirements can be grouped into five main categories:

- **Personal data governance and accountability:** Do you have effective policies and processes in place for collecting, storing, using, and sharing personal data, and for monitoring and proving compliance with those policies and processes?
- **Maintaining an inventory of personal data:** Do you know what, where, and whose personal data your organization holds at any given time?
- **Protecting personal data:** Are you ensuring the privacy, security, integrity, and availability of personal data and systems, both inside and outside your corporate walls?
- **Fulfilling individual rights requests:** Are you able to comply with individual requests for access, accuracy, erasure, portability, and processing of personal data?
- **Reporting data breaches:** Do you have effective processes in place to identify, assess, report on, and mitigate data breaches in a timely manner?

Thorough and continual compliance requires a combination of people, processes, and technologies from across the organization. From development, marketing, and analytics to legal, IT operations, and executive teams, everyone is responsible for protecting personal data and complying with the law.

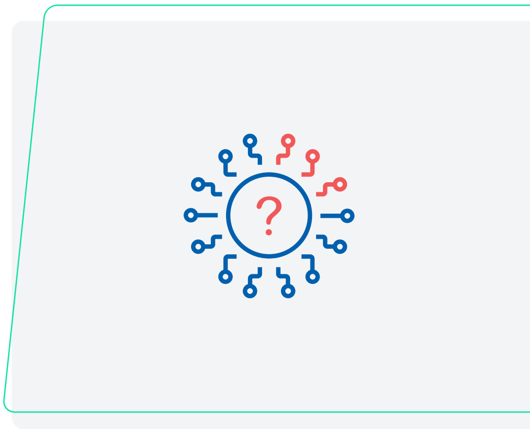
Your organization must have effective processes in place, as well as adherence to those processes, and documented proof of both. (Visit the PKWARE GDPR resource page to spot the holes in your enterprise compliance strategy.)

How Does PKWARE Make GDPR Compliance Easier?

Technology can certainly make compliance easier through automation, but there is no single technology solution that will make your organization “GDPR compliant.” PKWARE, however, offers a comprehensive suite of integrated technologies that can help get you there faster with a stronger footing. As always, we recommend consulting your legal or compliance teams to determine your compliance needs and risk posture, but from a technology perspective, PKWARE can help you address the following requirements of the GDPR.

Personal Data Inventory

Knowing and documenting the personal data your organization holds is the foundation of all GDPR compliance. It involves identifying and reporting the exact location of all personal data in your enterprise, in all its varied and vague formats, as well as the associated data subjects. PKWARE enables you to find all personal information, whether in the Cloud or on premises, both known and unknown. After scanning data repositories and systems, PKWARE provides a dashboard-level view of all personal data and identified risk exposure, with drill-down reports to the element level.



Data Protection

The existence of appropriate safeguards may help you retain personal data for business processing and will also reduce your compliance burden in the event of a data breach. The text of the GDPR was revised several times to include specific recommendations that organizations use encryption to protect personal information. PKWARE offers persistent encryption to ensure that any breached data remains unusable to unauthorized individuals. Because encrypted data remains safe even when stolen or misdirected, data controllers can avoid breach notification requirements and financial penalties under the GDPR, as well as other potentially catastrophic consequences of a data breach. PKWARE also offers pseudonymization, obfuscation, anonymization, and many other forms of masking to de-identify personal data while satisfying GDPR privacy requirements.

Data Minimization

Per Article 5 of the GDPR, data processing should only use as much data as is required to successfully accomplish a given task. Additionally, data collected for one purpose cannot be repurposed without further consent. The intent is to eliminate the unnecessary collection, processing, and storage of personal data and minimize the impact of a data breach. Depending on how the data is to be used, PKWARE can mask personal data in a realistic and consistent manner to maintain the data's business value, but remove any associated identity. PKWARE can also find and de-identify or delete data that has reached its retention limit or is not absolutely necessary. For example, analyzing purchasing trends does not necessarily require keeping complete credit card numbers; if still needed, the numbers could be partially masked to comply with GDPR.

Breach Detection and Reporting

Per Articles 33 and 34 of the GDPR, you will need to notify your supervisory data authority and/or affected data subjects within 72 hours of becoming aware of a high-risk data breach. As soon as possible, you should be able to pinpoint exactly which data was exposed, how and when the unauthorized access occurred, and the measures you have taken to mitigate adverse effects. PKWARE can alert data owners to unauthorized and/or unusual access to personal data in near real time to help organizations detect breaches in minutes, as well as provide details to assist in the analysis of the potential damage done by any breach.

In addition to the above aspects of GDPR, PKWARE can also help automate and enable the fulfillment of the following data subject rights requests:

Right of Access

Per Articles 13, 14, and 15 of the GDPR, the "right of access" mandate in the GDPR gives individuals the right to know what data you hold about them, along with how and why it is being used and accessed, and by whom. You must be able to retrieve and present this information within a reasonable time, not less than 30 days after an individual makes a request.

Gartner estimates that responding to a data subject rights request can cost more than $1,400 and take two to three weeks. With an up-to-date inventory of personal data and associated identities across the enterprise, PKWARE can automates the process, from capturing the initial request to creating a report that can be shared back with the individual.

Right of Erasure

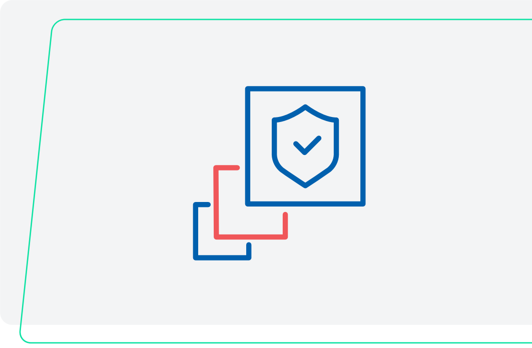
Upon request, and within what is allowed by the law, individuals can request an organization to erase all personal information about them. PKWARE supports the back-end processing and automated flows required for scalable implementations of this "right to erasure" (described in Article 17 of the GDPR) functionality.

Right to Data Portability

As a corollary to the right of access, the GDPR's Article 20 also requires personal data be made available in a machine-readable format that can then easily be transmitted to a different controller or processor, as requested by the data subject.

Right to Restrict Processing

Similar to the right to erasure, an individual can request an organization to restrict processing for a limited period of time until the issues related to processing are resolved. PKWARE supports the implementation of the "right to restrict processing" as described in Article 18 of the GDPR.



For many global organizations, the biggest challenge to complying with the GDPR's rules regarding data subject rights is the ability to keep track of all personal data everywhere—on premises, in the Cloud, and across the extended enterprise. To empower data subjects with the right to be forgotten, enterprises must not "forget" where personal data is located but rather maintain diligent visibility and control over it all. PKWARE can help.

Conclusion

GDPR compliance is not a one-time or even once-a-year requirement. Your enterprise will need to maintain a constant state of compliance—no small feat as big data gets bigger, cloud usage grows, and more users access more data for greater business insights. Personal data will be flowing continually into and out of your enterprise.

PKWARE can help you discover, protect, and monitor sensitive data in real-time, continuous processes, while providing your executives one consolidated view of compliance and risk positions at any given time. For more information visit: pkware.com.

[1] https://www.dlapiper.com/en/us/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/

[2] https://www.cpomagazine.com/data-protection/european-regulators-have-imposed-245-3-million-in-gdpr-fines-to-date-39-more-issued-in-2020/

[3] Ibid.

[4] https://www.gartner.com/en/newsroom/press-releases/2020-10-05-gartner-identifies-the-legal-and-compliance-technologies-to-focus-on-post-covid-19

Enterprise-Wide Policy Management

PK Protect provides a point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it’s copied or shared outside organizations

Integrated Discovery, Classification, and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance.
To learn more, visit PKWARE.com.

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204